

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-289255

(43) 公開日 平成11年(1999)10月19日

(51) Int.Cl.⁸

識別記号

F I

H 0 3 M 7/00

H 0 3 M 7/00

G 0 9 C 5/00

G 0 9 C 5/00

G 1 1 B 20/10

G 1 1 B 20/10

H

H 0 4 N 1/387

H 0 4 N 1/387

審査請求 未請求 請求項の数35 O L (全 20 頁)

(21) 出願番号 特願平11-14937

(22) 出願日 平成11年(1999)1月22日

(31) 優先権主張番号 特願平10-18667

(32) 優先日 平10(1998)1月30日

(33) 優先権主張国 日本 (J P)

(71) 出願人 000001007

キヤノン株式会社

東京都大田区下丸子3丁目30番2号

(72) 発明者 岩村 恵市

東京都大田区下丸子3丁目30番2号 キヤ
ノン株式会社内

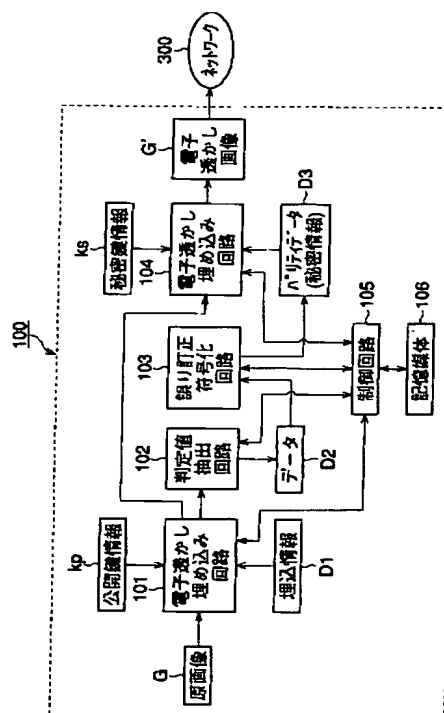
(74) 代理人 弁理士 國分 孝悦

(54) 【発明の名称】 電子機器、データ処理方法、電子透かし方式、データ処理システム、及び記憶媒体

(57) 【要約】

【課題】 一般のユーザによる自由な電子透かし情報の抽出と、デジタルデータの著作権の保護とを同時に満たすことが可能な著作権保護技術を用いたデータ処理システムを提供する。

【解決手段】 第1の埋込手段101は、公開鍵kpを用いて第1の情報D1をデジタルデータGに対して埋め込む。第2の埋込手段104は、第1の情報D1を復元するための第2の情報D3を埋め込む。この結果(デジタルデータG')の受取側は、公開鍵kpを用いてデジタルデータG'から第1の情報D1を自由に抽出することができ、デジタルデータG'の第1の情報D1が破壊されていたとしても、これを第2の情報D3によって復元することができる。



【特許請求の範囲】

【請求項 1】 デジタルデータに対して第 1 の情報を埋め込む第 1 の埋込手段と、上記第 1 の情報を復元するための第 2 の情報を上記デジタルデータに対して埋め込む第 2 の埋込手段とを備えることを特徴とする電子機器。

【請求項 2】 上記第 1 の情報及び上記第 2 の情報の埋込対象となる上記デジタルデータは、複数の領域に分割されており、それぞれの領域間に所定の関係を有することを特徴とする請求項 1 記載の電子機器。

【請求項 3】 上記複数の領域は、上記第 1 の情報が埋め込まれる第 1 の領域と、上記第 2 の情報が埋め込まれる第 2 の領域と、上記第 1 及び第 2 の情報が埋め込まれない第 3 の領域とを含むことを特徴とする請求項 2 記載の電子機器。

【請求項 4】 上記第 2 の情報は、上記第 1 の領域及び上記第 3 の領域から検出される各データに基づいて生成されることを特徴とする請求項 3 記載の電子機器。

【請求項 5】 上記複数の領域は、複数の実空間領域と複数の周波数領域の何れかの領域を含むことを特徴とする請求項 2 記載の電子機器。

【請求項 6】 上記第 2 の情報は、誤り訂正符号化処理によって生成されることを特徴とする請求項 1 記載の電子機器。

【請求項 7】 上記第 1 の情報は、上記デジタルデータの著作権を管理するための情報及び保護するための情報の少なくとも何れかの情報を含むことを特徴とする請求項 1 記載の電子機器。

【請求項 8】 上記第 1 の埋込手段は、離散コサイン変換、フーリエ変換、及びウェーブレット変換の少なくとも 1 つを用いて上記第 1 の情報を埋め込むことを特徴とする請求項 1 記載の電子機器。

【請求項 9】 上記第 1 の埋込手段は、上記デジタルデータが有する変数を操作することによって上記第 1 の情報を埋め込むことを特徴とする請求項 1 記載の電子機器。

【請求項 10】 上記変数は、デジタル画像データの輝度成分を含むことを特徴とする請求項 9 記載の電子機器。

【請求項 11】 上記第 1 の埋込手段での上記第 1 の情報を埋め込む方法と、上記第 2 の埋込手段での上記第 2 の情報を埋め込む方法とが異なることを特徴とする請求項 1 記載の電子機器。

【請求項 12】 上記第 1 の情報を埋め込むために必要な鍵情報が公開されていることを特徴とする請求項 1 記載の電子機器。

【請求項 13】 上記第 2 の情報を埋め込むために必要な鍵情報が公開されていないことを特徴とする請求項 1 記載の電子機器。

【請求項 14】 パーソナルコンピュータ、デジタル

カメラ、デジタルビデオレコーダ、カメラ一体型デジタルレコーダ、スキャナ、及び画像ファイル装置の少なくとも 1 つに備えたことを特徴とする請求項 1 記載の電子機器。

【請求項 15】 上記デジタルデータは、画像データを含むことを特徴とする請求項 1 記載の電子機器。

【請求項 16】 上記デジタルデータは、音声データ、グラフィックスデータ、テキストデータ、及びプログラムデータの少なくとも 1 つを含むことを特徴とする請求項 1 記載の電子機器。

【請求項 17】 デジタルデータに対して第 1 の情報を埋め込む第 1 の埋込ステップと、上記第 1 の情報を復元するための第 2 の情報を上記デジタルデータに対して埋め込む第 2 の埋込ステップとを含むことを特徴とするデータ処理方法。

【請求項 18】 第 1 の情報と、該第 1 の情報を復元するための第 2 の情報とが埋め込まれたデジタルデータから該第 2 の情報を抽出する抽出手段と、上記抽出手段にて得られた上記第 2 の情報に基づいて、上記第 1 の情報を復元する復元手段とを備えることを特徴とする電子機器。

【請求項 19】 第 1 の情報と、該第 1 の情報を復元するための第 2 の情報とが埋め込まれたデジタルデータから該第 2 の情報を抽出する抽出ステップと、上記抽出ステップにより得られた上記第 2 の情報に基づいて、上記第 1 の情報を復元する復元ステップとを含むことを特徴とするデータ処理方法。

【請求項 20】 デジタルデータを入力する入力手段と、公開された鍵情報を用いて上記デジタルデータに所定の情報を埋め込む埋込手段とを備えることを特徴とする電子機器。

【請求項 21】 上記所定の情報を復元するための秘密情報を上記デジタルデータに埋め込む手段を更に備えることを特徴とする請求項 20 記載の電子機器。

【請求項 22】 デジタルデータを入力する入力ステップと、公開された鍵情報を用いて上記デジタルデータに所定の情報を埋め込む埋込ステップとを含むことを特徴とするデータ処理方法。

【請求項 23】 上記所定の情報を復元するための秘密情報を上記デジタルデータに埋め込むステップを更に含むことを特徴とする請求項 22 記載のデータ処理方法。

【請求項 24】 デジタルデータを入力する入力手段と、公開された鍵情報を用いて上記デジタルデータから所定の情報を抽出する抽出手段とを備えることを特徴とする電子機器。

【請求項 25】 上記デジタルデータから検出される

秘密情報に基づいて、上記所定の情報を復元する復元手段を備えることを特徴とする請求項24記載の電子機器。

【請求項26】 デジタルデータを入力する入力ステップと、

公開された鍵情報を用いて上記デジタルデータから所定の情報を抽出する抽出ステップとを含むことを特徴とするデータ処理方法。

【請求項27】 上記デジタルデータから検出される秘密情報に基づいて、上記所定の情報を復元する復元ステップを含むことを特徴とする請求項26記載のデータ処理方法。

【請求項28】 公開された鍵情報を用いて、デジタルデータに所定の情報を埋め込む第1の装置と、
上記公開された鍵情報を用いて、上記デジタルデータに埋め込まれた所定の情報を抽出する第2の装置とを含むことを特徴とするデータ処理システム。

【請求項29】 上記第1の装置は、上記所定の情報を復元するための秘密情報を上記デジタルデータに埋め込み、

上記第2の装置は、上記秘密情報に基づいて、上記所定の情報を復元することを特徴とする請求項28記載のデータ処理システム。

【請求項30】 上記所定の情報は、上記デジタルデータの著作権を管理するための情報及び保護するための情報の少なくとも何れかの情報を含むことを特徴とする請求項28記載のデータ処理システム。

【請求項31】 著作権保護システムに備えたことを特徴とする請求項28記載のデータ処理システム。

【請求項32】 電子商取引システム及びデジタルデータ配布システムの少なくとも何れかのシステムに備えたことを特徴とする請求項28記載のデータ処理システム。

【請求項33】 デジタルデータに対して第1の情報を埋め込む第1の埋込工程と、
上記第1の情報を復元するための第2の情報を上記デジタルデータに対して埋め込む第2の埋込工程とを実現するためのプログラムを、コンピュータから読出可能に記憶したことを特徴とする記憶媒体。

【請求項34】 第1の情報と、該第1の情報を復元するための第2の情報とが埋め込まれたデジタルデータから該第2の情報を抽出する抽出工程と、
上記抽出工程により抽出された上記第2の情報に基づいて、上記第1の情報を復元する復元工程とを実現するためのプログラムを、コンピュータから読出可能に記憶したことを特徴とする記憶媒体。

【請求項35】 公開鍵を用いた電子透かし埋込処理により、原データに情報を埋め込む埋込工程と、
上記公開鍵を用いて、上記原データに埋め込まれた情報を抽出する抽出工程との少なくとも何れかの工程を含む

ことを特徴とする電子透かし方式。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、電子機器、データ処理方法、データ処理システム、及びコンピュータ読出可能な記憶媒体に関し、例えば、各種のデジタル情報の著作権を保護するための技術、或いは著作権を保護するための技術を用いたデジタル情報配布システムや電子商取引システムに適用される電子機器、データ処理方法、データ処理システム、及びそれを実施するための処理ステップをコンピュータが読出可能に格納した記憶媒体に関するものである。

【0002】

【従来の技術】近年のコンピュータネットワークの発達や、安価で高性能なコンピュータの普及により、近い将来、ネットワーク上で商品の売買を行うサービスである所謂「電子商取引」が盛んになると考えられている。この電子商取引で売買される商品は、例えば、静止画像等のデジタルデータである。しかしながら、電子商取引を実現するためには、解決しなければならない問題がいくつかある。その一つとして、例えば、デジタルデータは一般的に、完全なコピーを容易且つ大量に作成でき、その内容の変更も簡単にできるという性質を持っている。このため、デジタルデータからなる商品を買ったユーザが、オリジナルと同質のコピーデータ（複製）を不正に作成し、それを他のユーザに再配布してしまう可能性がある。この場合、その商品の著作権者又はその著作権者から正当に販売を委託された者（以下、「販売者」と言う）は、その商品に支払われるべき代価を受け取ることができないという問題が生じてくる。

【0003】一方、著作権者又は販売者（以下、デジタルデータからなる商品を正当に配布する側をまとめて「サーバ」と言う）が、一度購入者に対して商品を送ってしまうと、その商品の不正なコピーや内容の改ざん等を完全に防止することができないため、その商品の著作権が侵害されるという問題が生じてくる。そこで、このような電子商取引上の問題を解決する技術として、現在、「電子透かし」と呼ばれる技術が研究されている。

「電子透かし」とは、オリジナルのデジタルデータにある操作を加え、デジタルデータに関する著作権情報や購入者に関するユーザ情報を、デジタルデータ自体に目に見えないように埋め込む技術である。この技術を応用することによって、例えば、不正コピーが発見された場合に、誰がその不正コピーを再配布したのかを特定することができる。また、「電子透かし」の技術を実現する手法としては、現在、離散コサイン変換、フーリエ変換、ウェーブレット変換等を用いて、ある特定の周波数領域を操作する手法や、画素の輝度値を直接操作する手法が研究されている。

【0004】上述のような電子透かし技術の安全性と信

頼性は、デジタルデータに埋め込まれた情報が不可視であるということと、その情報の埋め込み場所と埋め込み強度とに関する鍵情報がわからなければ、その情報を破壊したり、内容を変更したりすることができないということとから成り立っている。例えば、「B. Pfitmann and M. Waidner : Asymmetric Fingerprinting, EUROCRYPT 96」には、画像毎に、その画像を購入したユーザの情報を埋込情報として埋め込むことで、不正配布を特定できるシステムが提案されている。しかしながら、このようなシステムにおいても、上記の埋込情報の鍵情報が公開されれば、不正なユーザはその埋込情報を破壊したり、変形したりすることができてしまう。このような問題を解決するために、次のような構成が考えられている。

【0005】まず、図14は、電子透かし技術を用いたシステム900の一例を示したものである。この図14において、埋込側910の電子透かし埋め込み回路911は、鍵情報kを用いてオリジナルの画像データGに埋込情報Dを埋め込む。ここで、鍵情報kは、埋込情報Dを抽出するために必要な情報であって、例えば、埋込情報Dの埋め込み場所や埋め込み強度等の情報である。埋込情報Dの埋め込まれた画像データGは、電子透かし画像データとして外部に送出される。一方、抽出側920の電子透かし抽出回路921は、埋込側910の鍵情報kと同じ鍵情報kを用いて、上記の電子透かし画像データから埋込情報Dを抽出する。このように、上記図14のシステム900では、埋込側910と抽出側920とで共通の鍵情報kを用いて、電子透かしである埋込情報Dの埋込及び抽出を行うように構成されている。

【0006】そこで、上記図14のシステム900において、上述した不正な処理を防止するためには、埋込情報Dの埋め込み場所や埋め込み強度等に関する鍵情報kを、埋込側910と抽出側920の何れにおいても秘密に保つ必要がある。このため、上記図14のシステム900では、埋込情報Dの抽出を、鍵情報kを生成した鍵情報管理機関や、鍵情報kを知ることのできる特別な検査機関においてのみ行うように構成することが考えられている。したがって、これらの機関が、不正に再配布されたデジタルデータや内容の変更されたデジタルデータを監視することによって、著作権者の権利の保護を実現することができる。

【0007】尚、上記図14に示したようなシステム900の構成は、暗号化技術のアナロジーで考えると、暗号化を行うための暗号鍵とその暗号化を復号するための復号鍵とが同じ鍵となる共通鍵暗号化方式的な手法による構成であると言える。

【0008】

【発明が解決しようとする課題】しかしながら、上記図14のシステム900では、埋込情報Dを抽出するために必要な鍵情報kを、埋め込み側910と抽出側920

とで共に秘密に管理する必要があったため、ネットワークを介して自由に送受信することはできなかった。また、埋込情報Dの抽出は、上述したような特殊な機関のみでしか行うことができないように構成されていた。したがって、一般の各ユーザは、埋込情報Dを自由に抽出することができなかったため、外部から入手したデジタルデータの著作権の内容やその正当性を確認することができず、大変不便であるという問題があった。

【0009】上記の問題を解決するためには、例えば、埋込情報Dを抽出するために必要な鍵情報kを、抽出側920の電子機器を製造するメーカを含めた一般のユーザに対して公開する必要がある。しかしながら、このような構成、すなわち鍵情報kを公開する構成とすれば、上述したような不正な処理によってデジタルデータの著作権が損なわれる恐れがある。つまり、単に鍵情報kを公開するだけでは、一般のユーザの誰もが自由に埋込情報Dを確認することはできるが、埋込情報Dによってデジタルデータの著作権を十分に保護することはできない。

【0010】上述のように、従来の電子透かし技術では、電子透かしである埋込情報Dの抽出に必要な鍵情報kを秘密に管理することなく、一般のユーザによる自由な電子透かしの抽出とデジタルデータの著作権の保護とを同時に満たすことのできる手法は提案されていなかった。また、このような電子透かし技術を適用した著作権保護のための技術も、その著作権保護技術を用いて構成された電子商取引システムやデジタル情報配布システムも提案されていなかった。

【0011】そこで、本発明は、上記の欠点を除去するために成されたもので、一般のユーザによる自由な電子透かし情報の抽出と、デジタルデータの著作権の保護とを同時に満たすことが可能な著作権保護技術を用いた電子機器、データ処理方法、データ処理システム、及びそれを実施するための処理ステップをコンピュータが読出可能に格納した記憶媒体を提供することを目的とする。

【0012】

【課題を解決するための手段】斯かる目的下において、第1の発明は、デジタルデータに対して第1の情報を埋め込む第1の埋込手段と、上記第1の情報を復元するための第2の情報を上記デジタルデータに対して埋め込む第2の埋込手段とを備えることを特徴とする。

【0013】第2の発明は、上記第1の発明において、上記第1の情報及び上記第2の情報の埋込対象となる上記デジタルデータは、複数の領域に分割されており、それぞれの領域間に所定の関係を有することを特徴とする。

【0014】第3の発明は、上記第2の発明において、上記複数の領域は、上記第1の情報が埋め込まれる第1の領域と、上記第2の情報が埋め込まれる第2の領域

7

と、上記第 1 及び第 2 の情報が埋め込まれない第 3 の領域とを含むことを特徴とする。

【0015】第 4 の発明は、上記第 3 の発明において、上記第 2 の情報は、上記第 1 の領域及び上記第 3 の領域から検出される各データに基づいて生成されることを特徴とする。

【0016】第 5 の発明は、上記第 2 の発明において、上記複数の領域は、複数の実空間領域と複数の周波数領域の何れかの領域を含むことを特徴とする。

【0017】第 6 の発明は、上記第 1 の発明において、上記第 2 の情報は、誤り訂正符号化処理によって生成されることを特徴とする。

【0018】第 7 の発明は、上記第 1 の発明において、上記第 1 の情報は、上記デジタルデータの著作権を管理するための情報及び保護するための情報の少なくとも何れかの情報を含むことを特徴とする。

【0019】第 8 の発明は、上記第 1 の発明において、上記第 1 の埋込手段は、離散コサイン変換、フーリエ変換、及びウェーブレット変換の少なくとも 1 つを用いて上記第 1 の情報を埋め込むことを特徴とする。

【0020】第 9 の発明は、上記第 1 の発明において、上記第 1 の埋込手段は、上記デジタルデータが有する変数を操作することによって上記第 1 の情報を埋め込むことを特徴とする。

【0021】第 10 の発明は、上記第 9 の発明において、上記変数は、デジタル画像データの輝度成分を含むことを特徴とする。

【0022】第 11 の発明は、上記第 1 の発明において、上記第 1 の埋込手段での上記第 1 の情報を埋め込む方法と、上記第 2 の埋込手段での上記第 2 の情報を埋め込む方法とが異なることを特徴とする。

【0023】第 12 の発明は、上記第 1 の発明において、上記第 1 の情報を埋め込むために必要な鍵情報が公開されていることを特徴とする。

【0024】第 13 の発明は、上記第 1 の発明において、上記第 2 の情報を埋め込むために必要な鍵情報が公開されていないことを特徴とする。

【0025】第 14 の発明は、上記第 1 の発明において、パーソナルコンピュータ、デジタルカメラ、デジタルビデオレコーダ、カメラ一体型デジタルレコーダ、スキャナ、及び画像ファイル装置の少なくとも 1 つに適用されたものであることを特徴とする。

【0026】第 15 の発明は、上記第 1 の発明において、上記デジタルデータは、画像データを含むことを特徴とする。

【0027】第 16 の発明は、上記第 1 の発明において、上記デジタルデータは、音声データ、グラフィックスデータ、テキストデータ、及びプログラムデータの少なくとも 1 つを含むことを特徴とする。

【0028】第 17 の発明は、デジタルデータに対し

8

て第 1 の情報を埋め込む第 1 の埋込ステップと、上記第 1 の情報を復元するための第 2 の情報を上記デジタルデータに対して埋め込む第 2 の埋込ステップとを含むことを特徴とする。

【0029】第 18 の発明は、第 1 の情報と、該第 1 の情報を復元するための第 2 の情報とが埋め込まれたデジタルデータから該第 2 の情報を抽出する抽出手段と、上記抽出手段にて得られた上記第 2 の情報に基づいて、上記第 1 の情報を復元する復元手段とを備えることを特徴とする。

【0030】第 19 の発明は、第 1 の情報と、該第 1 の情報を復元するための第 2 の情報とが埋め込まれたデジタルデータから該第 2 の情報を抽出する抽出ステップと、上記抽出ステップにより得られた上記第 2 の情報に基づいて、上記第 1 の情報を復元する復元ステップとを含むことを特徴とする。

【0031】第 20 の発明は、デジタルデータを入力する入力手段と、公開された鍵情報を用いて上記デジタルデータに所定の情報を埋め込む埋込手段とを備えることを特徴とする。

【0032】第 21 の発明は、上記第 20 の発明において、上記所定の情報を復元するための秘密情報を上記デジタルデータに埋め込む手段を更に備えることを特徴とする。

【0033】第 22 の発明は、デジタルデータを入力する入力ステップと、公開された鍵情報を用いて上記デジタルデータに所定の情報を埋め込む埋込ステップとを含むことを特徴とする。

【0034】第 23 の発明は、上記第 22 の発明において、上記所定の情報を復元するための秘密情報を上記デジタルデータに埋め込むステップを更に含むことを特徴とする。

【0035】第 24 の発明は、デジタルデータを入力する入力手段と、公開された鍵情報を用いて上記デジタルデータから所定の情報を抽出する抽出手段とを備えることを特徴とする。

【0036】第 25 の発明は、上記第 24 の発明において、上記デジタルデータから検出される秘密情報に基づいて、上記所定の情報を復元する復元手段を備えることを特徴とする。

【0037】第 26 の発明は、デジタルデータを入力する入力ステップと、公開された鍵情報を用いて上記デジタルデータから所定の情報を抽出する抽出ステップとを含むことを特徴とする。

【0038】第 27 の発明は、上記第 26 の発明において、上記デジタルデータから検出される秘密情報に基づいて、上記所定の情報を復元する復元ステップを含むことを特徴とする。

【0039】第 28 の発明は、公開された鍵情報を用いて、デジタルデータに所定の情報を埋め込む第 1 の装

置と、上記公開された鍵情報を用いて、上記デジタルデータに埋め込まれた所定の情報を抽出する第2の装置とを含むことを特徴とする。

【0040】第29の発明は、上記第28の発明において、上記第1の装置は、上記所定の情報を復元するための秘密情報を上記デジタルデータに埋め込み、上記第2の装置は、上記秘密情報に基づいて、上記所定の情報を復元することを特徴とする。

【0041】第30の発明は、上記第28の発明において、上記所定の情報は、上記デジタルデータの著作権を管理するための情報及び保護するための情報の少なくとも何れかの情報を含むことを特徴とする。

【0042】第31の発明は、上記第28の発明において、著作権保護システムに備えたことを特徴とする。

【0043】第32の発明は、上記第28の発明において、電子商取引システム及びデジタルデータ配布システムの少なくとも何れかのシステムに備えたことを特徴とする。

【0044】第33の発明は、デジタルデータに対して第1の情報を埋め込む第1の埋込工程と、上記第1の情報を復元するための第2の情報を上記デジタルデータに対して埋め込む第2の埋込工程とを実現するためのプログラムを、コンピュータから読出可能に記憶したことを特徴とする。

【0045】第34の発明は、第1の情報と、該第1の情報を復元するための第2の情報とが埋め込まれたデジタルデータから該第2の情報を抽出する抽出工程と、上記抽出工程により抽出された上記第2の情報に基づいて、上記第1の情報を復元する復元工程とを実現するためのプログラムを、コンピュータから読出可能に記憶したことを特徴とする。

【0046】第35の発明は、公開鍵を用いた電子透かし埋込処理により、原データに情報を埋め込む埋込工程と、上記公開鍵を用いて、上記原データに埋め込まれた情報を抽出する抽出工程との少なくとも何れかの工程を含む電子透かし方式であることを特徴とする。

【0047】

【発明の実施の形態】以下、本発明の実施の形態について図面を用いて説明する。

【0048】（第1の実施の形態）本発明は、例えば、図1に示すような電子機器（以下、「埋込装置」と言う）100と、図2に示すような電子機器（以下、「抽出装置」と言う）200とを含むシステムに適用される。埋込装置100は、詳細は後述する電子透かし埋め込み機能を有するものであり、抽出装置200も、詳細は後述する電子透かし抽出機能を有するものである。これらの装置は、公衆回線、インターネット、イーサネット等からなるネットワーク300を介して接続されている。以下、本実施の形態における埋込装置200及び抽出装置300の各構成、及びそれらの処理動作について

具体的に説明する。

【0049】〔埋込装置100の構成〕

【0050】上記図1の埋込装置100は、パーソナルコンピュータ、デジタルカメラ、デジタルビデオレコーダ、カメラ一体型デジタルレコーダ、スキャナ等の電子機器、或いはこれらの電子機器に接続可能な拡張ユニットである。上記図1に示すように、埋込装置100は、デジタル画像データ（原画像データ）G、公開鍵情報kp、及び埋込情報D1が供給される電子透かし埋込回路101と、電子透かし埋込回路101の出力が供給される判定値抽出回路102と、判定値抽出回路102の出力（＝データD2）が供給される誤り訂正符号化回路103と、誤り訂正符号化回路103の出力（＝パリティデータD3）、秘密鍵情報ks、及び電子透かし埋込回路101の出力（原画像データG＋埋込情報D1）が供給される電子透かし埋込回路104とを含んでなる。また、埋込装置100は更に、詳細は後述する本実施の形態における埋込処理に従って埋込装置100全体の動作を制御する制御回路105と、上記の埋込処理を実現するためのプログラムコードを記憶した記憶媒体106とを含んでなる。

【0051】ここで、公開鍵情報kpは、埋込情報D1を埋め込むために必要な情報（例えば、埋め込み場所や埋め込み手順を示す）であり、一般に公開されている鍵情報である。例えば、この公開鍵情報kpは、ネットワーク300に接続された電子機器の電子掲示板やホームページ等によって公開される。また、原画像データGは、ここでは静止画像や動画のデータとしている。但し、原画像データGとしては、静止画像や動画のデータに限られることはなく、例えば、音声、テキストデータ、グラフィックスデータ、プログラムデータ等のデジタルデータであってもよい。また、埋込情報D1は、電子透かし情報であって、原画像データGの著作権を保護したり管理するためのデータである。

【0052】〔抽出装置200の構成〕

【0053】上記図2の抽出装置200は、パーソナルコンピュータ、デジタルテレビ等の電子機器、或いはこれらの電子機器に接続可能な拡張ユニットである。上記図2に示すように、抽出装置200は、埋込情報D1の埋め込まれた電子透かし画像データGを入力する電子透かし抽出回路201と、電子透かし抽出回路201の出力（＝符号系列D4）が供給される誤り訂正復号回路202と、誤り訂正復号回路202の出力（＝訂正系列D5）が供給される電子透かし抽出回路203を含んでなる。また、抽出装置200は更に、詳細は後述する本実施の形態における抽出処理に従って抽出装置200全体の動作を制御する制御回路205と、上記の埋込処理を実現するためのプログラムコードを記憶した記憶媒体206とを含んでなる。

【0054】〔埋込装置100の処理動作〕

【0055】先ず、電子透かし埋込回路101は、公開鍵情報kpを用いて原画像データGを操作し、埋込情報D1を埋め込む。

【0056】ここで、本実施の形態では、埋込情報D1を抽出するための公開鍵情報kpは、上述したように一般に公開されているため、上述した特殊な機関（鍵情報を生成した鍵情報管理機関や、鍵情報を知ることのできる特別な検査機関等）のみならず、一般のユーザの誰でもが埋込情報D1の埋め込み位置、埋め込み強度、埋め込み手順等を知ることができると共に、その公開鍵情報kpに基づいて埋込情報D1を抽出し、その内容を確認することもできる。尚、公開鍵情報kpは、埋込装置100が外部のネットワーク300を介して入手する、或いは埋込装置100内部に予め格納されているものとする。ところが、公開鍵情報kpを公開した場合、不正なユーザが埋込情報D1を破壊したり、内容を変更したりすることによって、原画像データGの著作権が損なわれる恐れがある。

【0057】そこで、本実施の形態での埋込装置100は、埋込情報D1の破壊や内容の変更を防止するために、後述する誤り訂正符号化回路103及び電子透かし埋め込み回路104によって、「秘密情報」を生成して原画像データGに対して更に埋め込むようになされている。この秘密情報とは、埋込情報D1を修復するための情報であり、これを用いることによって、抽出装置200は、破壊、変形、加工された埋込情報D1を修復することができるようになされている。ここでの埋込情報D1の修復は、例えば、誤り訂正符号化と復号の手法によって実現することができる。この場合、例えば、上記の秘密情報を、埋込情報D1を埋め込んだ部分（以下、「公開情報埋込部」と言う）と、埋込情報D1も秘密情報をも埋め込まない部分（以下、「無情報埋込部」と言う）とから検出されたデータを用いて生成する。また、秘密情報の修復については、公開情報埋込部、秘密情報を埋め込む部分（以下、「秘密情報埋込部」と言う）、及び無情報埋込部の3つの領域から検出されたデータを直接用いて実行される。

【0058】尚、上述の秘密情報の生成に無情報埋込部から検出されたデータを用いるのは、該秘密情報が原画像データGのどこに埋め込まれているのかを特定できないようにするためである。

【0059】次に、判定値抽出回路102は、電子透かし埋込回路101にて埋込情報D1が埋め込まれた原画像データG（原画像データG+埋込情報D1）から2つの領域を判別する。すなわち、公開情報埋込部と公開情報埋込部以外の部分を判別する。また、判定値抽出回路102は、所定の規則に基づいて、公開情報埋込部以外の部分から秘密情報埋込部と無情報埋込部を決定する。ここで、それぞれの埋込部の領域の大きさは、公開情報埋込部に埋め込まれる埋込情報D1の情報長、埋込情報

D1を復元するために必要な復元能力（ここでは、誤り訂正能力とする）等に応じて変化する。そして、判定値抽出回路102は、所定の規則に基づいて、公開情報埋込部と無情報埋込部からデータD2を検出し、このデータD2（埋込情報D1に対応する検出データを含む）を誤り訂正符号化回路103に供給する。

【0060】尚、判定値抽出回路102でのデータD2を生成する手順については後述する。また、判定値抽出回路102を電子透かし埋込回路101の後段に設けるように構成したが、詳細は後述するが、判定値抽出回路102を電子透かし埋込回路101の前段に設けるように構成してもよい。

【0061】次に、誤り訂正符号化回路103は、所定の誤り符号化処理により、判定値抽出回路102からのデータD2に対する誤り符号（パリティデータ）D3を生成し、これを上述した埋込情報D1を修復するための秘密情報D3として、電子透かし埋め込み回路104に供給する。

【0062】そして、電子透かし埋め込み回路104は、誤り訂正符号化回路103からの秘密情報D3（すなわち、パリティデータD3）を、判定値抽出回路102にて決定された秘密情報埋込部に埋め込み、これを電子透かし画像データG'として出力する。

【0063】上述のようにして、埋込装置100は、原画像データGを操作することによって、埋込情報D1と秘密情報D3を埋め込んだ電子透かし画像データG'（G+D1+D3）を生成する。この電子透かし画像データG'は、ネットワーク300を介して抽出装置200に供給される。

【0064】〔抽出装置200の処理動作〕

【0065】先ず、電子透かし抽出回路201は、埋込装置100の埋め込み方法に対応する抽出方法に基づいて、詳細は後述するが、埋込装置100からネットワーク300を介して供給された電子透かし画像データG'から符号系列データD4（秘密情報D3を含む）を抽出し、それを誤り訂正復号回路202に供給する。このとき、電子透かし抽出回路201は、秘密に管理する必要のない公開鍵情報kpを用いて、電子透かし画像データG'から埋込情報D1のみを抽出することもできる。

【0066】尚、公開鍵情報kpは、抽出装置200が外部のネットワーク300を介して入手する、或いは抽出装置200の中に予め格納されているものとする。また、電子透かし抽出回路201での抽出方法は、埋込装置100の埋め込み方法に対応するものに限られず、他の方法を用いることも可能である。

【0067】次に、誤り訂正復号回路202は、電子透かし抽出回路201からの符号系列データD4（=D2+D3）に含まれるパリティデータD3（すなわち、秘密情報D3）を用いて、それに対応するデータD2を誤り訂正復号し、その結果を訂正系列データD5として電

子透かし抽出回路203に供給する。ここでの処理によって、埋込情報D1がたとえ破壊されていたとしても、復元することができる。

【0068】そして、電子透かし抽出回路203は、公開鍵情報kpを用いて、誤り訂正復号回路202からの訂正系列データD5から、埋込情報D1を検出する。

【0069】上述のような構成により、抽出装置300は、秘密情報D3を用いて電子透かし画像データG'から抽出された埋込情報D1を修復し、復元することができる。また、電子透かし抽出回路203にて検出された埋込情報D1を、次段に設けられている表示部204に供給することにより、電子透かし画像データG'の著作権情報やユーザ情報等を視覚的に確認することもできる。

【0070】したがって、本実施の形態での構成によれば、埋込情報D1を抽出するために必要な公開鍵情報kpを秘密に管理する必要がなくなり、誰でも自由に埋込情報D1を抽出でき、その内容を確認することができる。また、不正なユーザによって埋込情報D1が破壊されたり、変更されたとしても、上述の秘密情報D3を用いて埋込情報D1を復元することができるため、原画像データGの著作権を十分に保護することができ、埋込情報D1の信頼性と安全性を向上させることもできる。

【0071】尚、本実施の形態での抽出装置200において、更に、電子透かし抽出回路201により抽出された埋込情報D1と、電子透かし抽出回路203から抽出された埋込情報D1とを比較し、電子透かし画像データG'に埋め込まれている埋込情報D1が改竄されているか否かを検出するように構成してもよい。これにより、抽出装置200に改竄検出機能を付加することができ、電子透かし画像データG'の著作権保護をより一層高めることができる。また、改竄検出の結果を表示部204に供給することによって、電子透かし画像データG'の正当性をユーザに視覚的に通知することもできる。

【0072】また、抽出装置200に付加する改竄検出機能としては、上述の機能構成のものに限らず、例えば、符号系列データD4の誤りが、誤り訂正復号回路202の訂正能力を超えた場合（すなわち、誤り訂正不能となる場合）に、埋込情報D1が改竄されたと検出するようにしてもよい。これにより、抽出装置200に付加する改竄検出機能を、簡単に構成することができる。

【0073】〔埋込装置100での埋込手法、及び抽出装置200での抽出手法〕図3～5を用いて、埋込装置100に適用される埋込手法の一例と、抽出装置200に適用される抽出手法の一例とについて具体的に説明する。

【0074】（1）埋込方法

図3は、本実施の形態における埋込方法の手順を示したものである。

【0075】ステップS411：まず、埋込情報D1

を、上述した公開情報埋込部に埋め込む。すなわち、電子透かし埋込回路101は、公開鍵情報kpを用いて原画像データGを操作し、原画像データGに埋込情報D1を埋め込む。このとき、電子透かし埋込回路101は、所定の規則に従って、公開情報埋込部の画像データを操作する。上記の所定の規則とは、例えば、埋め込み対象となる変数を原画像データGの画素の輝度値とした場合、原画像データGの輝度の平均値（すなわち、全画素の輝度の平均値）Cと、図4に示すような、公開情報埋込部を構成するブロックの輝度の平均値 C_{ij} （縦方向i番目、横方向j番目のブロックを公開情報埋込部としたときの該ブロックの輝度の平均値）との間に予め設定された規則である。ここでは、あるブロックに“1”を埋め込む場合、「 $C \leq C_{ij}$ 」となるように、そのブロックの輝度の平均値 C_{ij} を操作する。また、あるブロックに“0”を埋め込む場合には、「 $C > C_{ij}$ 」となるように、そのブロックの輝度の平均値 C_{ij} を操作するものとする。したがって、上記図4において、公開情報埋込部となるブロックをC23及びC24とし、各ブロックに埋め込む埋込情報D1を{1, 0}とした場合、電子透かし埋込回路101は、 $C \leq C_{23}$ 、 $C > C_{24}$ となるように、各ブロックの輝度の平均値 C_{23} 及び C_{24} を操作することになる。ここで、各ブロックの操作の大きさは、埋め込み強度によって決定される。尚、公開情報埋込部となるブロックの位置及び埋め込み強度は、上述したような一般のユーザに公開することのできる情報である。

【0076】ステップS412～ステップS419：次に、秘密情報D3を埋め込む。例えば、情報の埋込の対象となる変数を、原画像データGの画素の輝度値とした場合、次のようなステップS412～ステップS419の処理が実行される。

【0077】まず、判定値抽出回路102は、原画像データGの輝度の平均値（以下、これを“C”で示す）を求める（ステップS412）。次に、判定値抽出回路102は、上記図5に示すように、原画像データGを複数のブロック（ここでは、 4×4 の16ブロック）に分割し（ステップS413）、それぞれのブロック毎の輝度の平均値 C_{ij} を求める（ステップS414）。そして、各ブロックの処理順を定める。ここでは、その処理順を、 C_{11} 、 C_{12} 、 C_{13} 、 C_{14} 、 C_{21} 、 C_{22} 、 \dots 、 C_{43} 、 C_{44} のブロックの順番とする。次に、判定値抽出回路102は、埋込情報D1の埋め込まれたブロック（すなわち、公開情報埋込部）を判別する（ステップS415）。ここで、公開情報埋込部の各ブロックには、ステップS411にて説明した規則に従って埋込情報D1が埋め込まれている。次に、判定値抽出回路102は、秘密情報D3を埋め込むブロック（すなわち、秘密情報埋込部）を決定し、埋込情報D1も秘密情報D3も埋め込まないブロック（すなわち、無情報埋込部）を決定する（ステップS416）。ここでは、上記図4において、

秘密情報埋込部を、 C_{31} , C_{32} , C_{33} , C_{34} , C_{41} , C_{42} , C_{43} , C_{44} のブロックとし、無情報埋込部を、 C_{11} , C_{12} , C_{13} , C_{14} , C_{21} , C_{22} のブロックとする。そして、判定値抽出回路102は、ステップS416にて決定した公開情報埋込部と無情報埋込部に対して、所定の判定処理を行い、データD2を検出する(ステップS417)。例えば、判定値抽出回路102は、各ブロックの輝度の平均値 C_{ij} に対して、「 $C \leq C_{ij}$ 」のとき $C_{ij} = "1"$ 、「 $C > C_{ij}$ 」のとき $C_{ij} = "0"$ とする判定処理を行い、所定の順番に従って、各ブロックから“1”又は“0”を検出する。この検出結果がデータD2となる。

【0078】尚、ここでは、公開情報埋込部に埋込情報D1を埋め込む規則と、公開情報埋込部と無情報埋込部からデータD2を検出する規則とを、同じ規則(すなわち、「 $C \leq C_{ij}$ 」のとき $C_{ij} = "1"$ 、「 $C > C_{ij}$ 」のとき $C_{ij} = "0"$ とする)としたが、これに限られるものではない。これらの規則の間に所定の関係(すなわち、データD2の一部が埋込情報D1と1対1に対応する関係)が成り立つのであれば、これらを全く逆の規則としてもよい。

【0079】上述のようにして、判定値抽出回路102において、公開情報埋込部と無情報埋込部の各ブロックから所定の規則に従って検出されたデータD2は、誤り訂正符号化回路103に供給される。誤り訂正符号化回路103は、判定値抽出回路102からのデータD2を誤り訂正符号化し、パリティデータD3を生成する(ステップS418)。ここでは、このパリティデータD3が上述の秘密情報となる。そして、電子透かし埋込回路104は、秘密鍵情報 k_s に基づいて、誤り訂正符号化回路103にて生成されたパリティデータD3を、判定値抽出回路102により決定された(ステップS416参照)秘密情報埋込部に埋め込む(ステップS419)。

【0080】ここで、電子透かし埋込回路104にて用いられる秘密鍵情報 k_s は、少なくとも秘密情報埋込部の位置が含まれる。この秘密鍵情報 k_s は、公開鍵情報 k_p と異なり一般に公開されることはない。ステップS419では、秘密情報D3の埋込規則を、秘密情報埋込部及び無情報埋込部からデータD2を検出する規則と同じとする。これにより、抽出装置200では、単一の規則により秘密情報D3とデータD2を抽出することができる。また、秘密情報D3の埋込規則を、公開情報D1の埋込規則と同じとすることにより、抽出装置200側の処理を更に簡略化することができる。

【0081】尚、ステップS419での埋め込み規則は、上述の規則と異なった規則であってもよい。例えば、上記図5において、無情報埋込部を $C_{11} \sim C_{22}$ のブロックとし、公開情報埋込部を C_{23} , C_{24} のブロックと

し、秘密情報埋込部を $C_{31} \sim C_{44}$ のブロックとした場合、電子透かし埋込回路104は、「 $C \leq C_{ij}$ 」となるようにそのブロックの輝度の平均値 C_{ij} を操作することにより“0”を埋め込む。また、「 $C > C_{ij}$ 」となるようにそのブロックの輝度の平均値 C_{ij} を操作することにより“1”を埋め込む。

【0082】また、誤り訂正符号化回路103にて用いる誤り訂正符号化方法としては、例えば、(15, 7, 5)のBCH符号(今井秀樹著、電子情報通信学会発行: “符号理論” 7. 1節参照)を採用するものとしてよい。この場合、符号長が $C_{12} \sim C_{44}$ のブロックから検出される“15”、情報長が $C_{12} \sim C_{24}$ のブロックから検出される“7”、最小距離が“5”となる誤り訂正符号が構成することができる。これにより、 $C_{31} \sim C_{44}$ の各ブロックには、 $C_{12} \sim C_{24}$ の各ブロックから検出されたデータに基づいて算出された8ビットのパリティデータD3が埋め込まれることになる。

【0083】さらに、誤り訂正符号化回路103にて用いる誤り訂正符号化方法としては、上述の(15, 7, 5)のBCH符号に限られず、例えば、各ブロックを更に細かく分割し、公開情報埋込部と秘密情報埋込部の少なくとも一方を大きくすることによって、誤り訂正能力をより向上させた誤り訂正符号化方法を採用するとしてもよい。

【0084】(2) 抽出手法

図5は、本実施の形態における抽出方法の手順を示したものである。

【0085】ステップS421: まず、抽出方法に必要な情報、すなわち公開情報埋込部として決定されたブロック(ここでは、 C_{23} 及び C_{24} の各ブロックとする)の位置、及び埋込情報D1の埋込規則と抽出規則は、公開鍵情報 k_p の一部として一般に公開されている。そこで、電子透かし抽出回路201は、埋込情報D1が埋め込まれたデジタル画像データ(すなわち、電子透かし画像データ G')を受け取り、上記図4に示したような複数のブロック(ここでは、 4×4 の16ブロック)に分割し、各ブロック毎の輝度の平均値 C_{ij} を求める。

【0086】ステップS422: 次に、電子透かし抽出回路201は、電子透かし画像データ G' の輝度の平均値(すなわち、全画素の輝度の平均値) C を求める。ここで、この平均値 C を、公開鍵情報 k_p の一部として公開するようにしてもよい。

【0087】ステップS423: 次に、電子透かし抽出回路201は、上記図4に示す全てのブロックに対して所定の規則に基づいた判定処理を行い、符号系列データD4を生成する。ここでの所定の規則とは、上述した(1)埋込方法と対応するものであり、例えば、各ブロックの輝度の平均値 C_{ij} に対して、「 $C \leq C_{ij}$ 」のとき $C_{ij} = "1"$ 、「 $C > C_{ij}$ 」のとき $C_{ij} = "0"$ とする規則である。各ブロックの判定結果は、予め定められた

ブロックの順番に従って並べられ、符号系列データD 4となる。この符号系列データD 4が、誤り訂正復号回路202に供給されることになる。

【0088】ステップS 424：誤り訂正復号回路202は、電子透かし抽出回路201からの符号系列データD 4を用いて、上述した(1)埋込方法の誤り訂正符号化方法に対応する誤り訂正復号を行う。この復号された符号系列データD 4は、訂正系列データD 5として電子透かし抽出回路203に供給される。ここで、例えば、公開情報埋込部であるC₂₃及びC₂₄の各ブロックに存在する情報に対して破壊、或いは画素値の変更や切り取り等が行われていた場合、上記の符号系列データD 4には、少なくとも2ビットの誤りを含むことになる。しかしながら、符号系列データD 4は、所定の方式(例えば、

(15, 7, 5)のBCH符号)に基づいて、誤り訂正符号化されているデータであるため、この方式に対応する復号処理を施せば、破壊や変更された少なくとも2ビットのデータを訂正し、復元することができる。したがって、この結果、誤り訂正復号回路302は、復元された符号系列データD 4(訂正系列データD 5)を得ることができる。

【0089】ステップS 425：電子透かし抽出回路203は、誤り訂正復号回路202からの訂正系列データD 5の中から、公開埋込情報D 1(或いは、公開埋込情報D 1と1対1に対応するデータ)を検出することによって、公開埋込情報D 1(例えば、{1, 0})を取得する。この結果、例え破壊されても、復元可能な範囲であれば、常に正しい公開埋込情報D 1が抽出装置200にて認識されることになる。ここで、公開埋込情報D 1は、公開鍵情報k_p(例えば、公開情報埋込部の位置)に基づいて、訂正系列データD 5の中から検出される。

【0090】尚、上述した(2)抽出方法では、少なくとも2ビットの誤りを訂正することのできる誤り訂正符号を抽出し、それを復号するものとしたが、これに限らず、例えば、ブロックの分割を更に細かくし、パリティデータの埋め込める秘密情報埋込部の領域を大きくすることで、2つ以上の誤りの訂正と、公開埋込情報D 1以外に生じた誤りの訂正とに対応させることもできる。

【0091】[(1)埋込手法、(2)抽出手法の応用例] 上述した(1)埋込方法と(2)抽出方法を応用することにより、埋込情報の耐性の向上、抽出情報の誤り訂正能力の向上、原画像の画質劣化の抑制等、様々な効果をもたらす埋込方法と抽出方法を構成することもできる。以下、図6及び図7を用いて、第1の実施の形態の変形例1～6を説明する。尚、図6及び図7において、上記図1での同様の構成或いは機能を有する処理部については同一の符号を付し、その詳細な説明を省略する。

【0092】(例1)：上記図1に示した埋込装置100では、埋込情報D 1を符号化することなく原画像データGに埋め込む構成について説明したが、これに限ら

ず、例えば、埋込情報D 1を誤り訂正符号化処理や、暗号化処理等の一方向性関数的な演算により符号化してもよい。

【0093】具体的には例えば、上記図1の埋込装置100において、図6(a)に示すように、誤り訂正符号化回路107を新たに設ける。この場合、誤り訂正符号化回路107は、上述の埋込情報D 1自体を誤り訂正符号化する。或いは、上記図1の埋込装置100において、上記図6(b)に示すように、公開鍵暗号方式の機能を有する暗号化回路108を新たに設けることも可能である。この場合、暗号化回路108は、上述の埋込情報D 1自体を、秘密鍵を用いて公開鍵暗号化する。さらに、上記図1の埋込装置100において、上記図6

(a)に示したような誤り訂正符号化回路107、及び同図(b)に示したような暗号化回路108を組み合わせた構成を新たに設けることも可能である。この場合、上述の埋込情報D 1には、誤り訂正符号化と暗号化が交互に施される。

【0094】ここで、上記の一方向性関数とは、関数 $y = f(x)$ において、 x から y を求めることは容易であるが、逆に y から x を求めることの困難な関数を言う。例えば、桁数の大きな整数に対する素因数分解や離散対数等が一方向性関数としてよく用いられる。このような一方向関数を用いて符号化する構成とする場合、埋込装置100の電子透かし埋込回路101には、誤り訂正符号化回路107により誤り訂正符号化された埋込情報D 1(すなわち、符号化埋込情報D 1')、暗号化回路108により暗号化された埋込情報D 1(すなわち、暗号化埋込情報D 1'')、及び誤り訂正符号化回路107と暗号化回路108の組合せにより符号化された埋込情報D 1の何れかの情報が、上記図1での埋込情報D 1の代わりに供給されることになる。このような構成とすることで、埋込情報D 1の耐性、埋込情報D 1の誤りを訂正する能力、埋込情報D 1の安全性と信頼性を向上させることができる。

【0095】尚、上記図1の埋込装置100を、上記図6(a)の構成、同図(b)の構成、或いはその両方を組み合わせた構成とした場合、抽出装置200を、その構成に対応した構成とすれば、抽出装置200は、埋込装置100にて符号化された埋込情報D 1を抽出し、復号することができる。

【0096】(例2)：上述した(1)埋込方法では、埋込情報D 1を符号化することなく、原画像データGの公開情報埋込部に埋め込むようにしたが、これに限らず、例えば、上記図6(a)に示したような構成を有する埋込装置100のように、埋込情報D 1を誤り訂正符号化したデータ(すなわち、埋込情報D 1')を、原画像データGの公開情報埋込部に埋め込むようにしてもよい。この場合、抽出装置200は、公開情報埋込部とその他の部分から検出された情報を復号し、誤りを検出

10

20

30

40

50

し、そして訂正する。このとき、公開情報埋込部から検出された情報（すなわち、埋込情報 D 1'）に誤りが検出された場合、抽出装置 200 において更に、その情報を復号し、消失訂正するように構成することもできる。これにより、誤り訂正能力をより一層向上させることができる。また、埋込情報 D 1 の復元をする能力をより一層向上させることもできるため、埋め込み情報の耐性を更に向上させることができる。

【0097】（例 3）：上述した（1）埋込方法において、公開情報埋込部及び秘密情報埋込部とするブロックの選択は任意であり、ランダムに選択可能であるが、その選択を次のようににしてもよい。

【0098】具体的には、まず、 C_{ij} の値が平均値 C に近いものは、圧縮や種々の変形によって値が変化しやすいため、情報の埋込時には「 $C \leq C_{ij}$ 」であっても、情報の抽出時には「 $C > C_{ij}$ 」となることが考えられる。このようなブロックが無情報埋込部として選択されると、抽出時にデータ D 2 が誤って検出される場合がある。そこで、例えば、耐性が弱い、すなわち C_{ij} の値が平均値 C に近いブロックを、埋込情報 D 1 又は秘密情報 D 3 を埋め込むブロックとし、それらのブロックを操作して、予めある程度の強度を持たせるようにする。これにより、圧縮や種々の変形に耐性のある電子透かし埋込方法を実現できる。また、この場合、 C_{ij} の値が平均値 C に近いブロックに対して、「 $C \leq C_{ij}$ 」又は「 $C > C_{ij}$ 」となるような操作を加えることになるため、その分変化量をほぼ半分程度に抑えることができ、したがって、画質劣化を小さくすることができる（例えば、平均値 C よりも非常に大きい値 C_{ij} を有するブロックに対して、「 $C > C_{ij}$ 」となるような操作を加える必要がある場合、このときの画質劣化は大きい）。

【0099】また、無情報埋込部となるブロックの選択については、埋込装置 100 の構成を、例えば、図 7 に示すように、判定値抽出回路 102 を電子透かし埋込回路 101 の前段に設け、判定値抽出回路 102 により、原画像データ G の各ブロックの判定値を予め抽出し、この判定値に基づいて、各情報を埋め込むブロックを決定するようにしてもよい。これにより、 C_{ij} の値が平均値 C に近いブロックを無情報埋込部として選択することができる。

【0100】上述のようなブロック選択のための構成により、電子透かし画像の画質劣化を更に小さく、且つ埋込情報 D 1 の耐性をより一層強化することができる。

【0101】（例 4）：上述した（1）埋込方法では、ブロックの順番を任意に定めることができるが、次のような構成によってブロックの順番を定め、秘密情報 D 3 を埋め込むようにしてもよい。例えば、上記図 7 の埋込装置 100 において、原画像データ G の各ブロックの輝度の平均値 C_{ij} を予め判定した後、その原画像データ G の各ブロックの判定値自体が、埋込情報 D 1 を復元する

ための秘密情報となるように各ブロックの順番を定める。この場合、情報の埋込を行う（すなわち、画像データに操作を加える）ブロックの数が略最小距離の数となり、原画像データ G や埋込情報 D 1 に係わらず略一定となる。

【0102】具体的には、上記図 7 の構成において、先ず、判定値抽出回路 102 は、原画像データ G のブロックの値を判定した後、平均値 C に近くない C_{ij} のブロックを無情報埋込部のブロックとして、任意にブロックの順番を定める。次に、判定値抽出回路 102 は、平均値 C に近い C_{ij} のブロックの一部を公開情報埋込部のブロックとして、任意にブロックの順番を定める。そして、誤り訂正符号化回路 103 は、判定値抽出回路 102 にて定められた順番に従って並べられた公開情報埋込部のブロックの判定値と、無情報埋込部のブロックの判定値とを、データ D 6 として誤り訂正符号化する。その後、誤り訂正符号化回路 103 は、データ D 6 のパリティデータ D 3 を秘密情報として電子透かし埋込回路 104 に供給する。電子透かし埋込回路 104 は、秘密情報埋込部（平均値 C に近い C_{ij} のブロックの一部）の判定値を用いて、各ブロックの順番をパリティデータ D 3 を構成する順番となるように定める。

【0103】したがって、上述のような構成とすることにより、原画像データ G を実際に操作することなく、秘密情報 D 3 の埋め込みを行うことができるため、操作を加えるブロックの数を小さく、且つ平均的にすることができる。また、原画像データ G の画質に与える影響をより一層抑制することもできる。

【0104】（例 5）：上述した（1）埋込方法では、原画像データ G から検出されたデータ D 2 を 1 つのデータとして符号化する（すなわち、データ D 2 を誤り訂正符号化する）ようにしたが、これに限らず、例えば、原画像データ G から検出されたデータ D 2 を複数の部分データに分割し、各部分データ毎に、又は重複を許す部分データ毎に、誤り訂正符号化するようにしてもよい。

【0105】（例 6）：上述した（1）埋込方法では、原画像データ G を複数のブロックに分割した後、各ブロックの輝度の平均値を操作することにより、埋込情報 D 1 及び秘密情報 D 3 の埋め込みを行うようにしたが、これに限られるものではない。また、上述した（1）埋込方法では、誤り訂正符号化方法として、（15, 7; 5）の BCH 符号化を採用するようにしたが、これに限られるものでもない。例えば、情報の埋め込みについては、ウェーブレット変換や離散コサイン変換等の周波数変換方式を用いて、1 つ以上のブロックを周波数変換し、所定の周波数領域に対して情報の埋め込みを行うようにしてもよい。或いは、フーリエ変換を用いてこれを行うようにしてもよい。或いは、画像の画素を操作することによって、空間領域に対する情報の埋め込みを行うようにしてもよい。尚、周波数変換方式を用いて埋込処

理を行う場合、公開情報D1と秘密情報D3とを異なる周波数領域に対して埋め込むようにしてもよい。

【0106】具体的には、例えば、フーリエ変換を用いる場合、原画像データG全体をフーリエ変換し、その変換値の中から耐性等に応じて、いくつかの情報を埋め込む部分の候補を決定し、その決定した部分の一部を公開情報埋込部（公開鍵情報kpに基づく情報埋め込み領域）とし、その他の部分を秘密情報埋込部（秘密鍵情報ksに基づく情報埋め込み領域）、或いは無情報埋込部（何も情報を埋め込まない領域）とすれば、本実施の形態での（1）埋込方法と同様の原理を応用することができる。このとき、上述の複数の異なる埋め込み方法を組合せ、埋込情報D1及び秘密情報D3を原画像データGに埋め込むように構成してもよい。

【0107】また、誤り訂正符号化方法としては、例えば、他のブロック符号化方式や、畳み込み符号化（木符号化）方式等、種々の誤り訂正符号化方式を採用することができる。

【0108】また、埋め込み対象となるデジタルデータについても、デジタル画像データに限らず、動画データ、テキストデータ、音声データ、グラフィックスデータ、プログラムデータ等、種々のデジタルデータを対象とすることができ、何れのデジタルデータに対しても、本実施の形態での埋込方法を応用することができ、また、埋込情報D1の埋め込みと抽出に必要な鍵情報を、一般に公開することができる。

【0109】上述したような、本実施の形態の変形例1～6によれば、埋め込み情報の耐性の向上、埋め込み情報を復元する能力（即ち、誤り訂正能力）の向上、原画像の画質劣化の抑制等、様々な効果をもたらす埋込方法と抽出方法とを提供することができる。

【0110】（第2の実施の形態）本実施の形態では、上述した第1の実施の形態における埋込装置100と抽出装置200を用いて構成されるシステムを、例えば、図8に示すような構成のシステムに適用する。このシステムは、公衆回線、インターネット、イーサネット等からなるネットワーク300を用いて構成されるシステムであって、例えば、静止画像データ、動画データ、音声データ、テキストデータ、グラフィックスデータ、プログラムデータ等のデジタルデータを配布したり、売買したりするデジタル情報配布システムや、電子商取引システム等に適用されるものである。以下、本実施の形態でのシステムについて具体的に説明する。

【0111】尚、上記図8に示す本実施の形態でのシステムにおいて、第1の実施の形態でのシステムと同様の構成或いは機能を有する部分については同一の符号を付し、その詳細な説明を省略する。

【0112】先ず、上述した第1の実施の形態と同様にして、埋込装置100は、公開鍵情報kpに基づいて、埋込情報D1を原画像データGに埋め込む。次に、埋込

装置100は、埋込情報D1を復元するために必要な秘密情報（第1の実施の形態では、パリティデータD3）を、原画像データGに埋め込む。そして、埋込装置100は、埋込情報D1及び秘密情報を埋め込んだ電子透かし画像データG'を、所定の手順（例えば、デジタル情報配布システムや電子商取引システムに基づく手順）に従って、ネットワーク300に対して送出する。

【0113】ここで、埋込装置100にて用いられる公開鍵情報kpは、一般に公開された情報であり、埋込装置100と抽出装置200との間で秘密に管理する必要がなく、また、埋込装置100と抽出装置200との間のネットワーク300を介して自由に送受信できる情報である。ここでは、公開鍵情報kpは、埋込装置100にて電子透かし画像データG'に付加されて、ネットワーク300に対して送出されるものとする。

【0114】一方、抽出装置200は、公開鍵情報kpに基づいて、ネットワーク300を介して供給された電子透かし画像データG'から、埋込情報D1を抽出する。このとき、上述した第1の実施の形態と同様に、抽出装置200は、電子透かし画像データG'に埋め込まれた秘密情報を用いて、埋込情報D1を復元することもできる。また、公開鍵情報kpに基づいて抽出された埋込情報D1と、秘密情報を用いて復元された埋込情報D1とを比較することにより、電子透かし画像データG'に対する改竄を検出することもできる。

【0115】したがって、本実施の形態によれば、上述した第1の実施の形態と同様に、埋込情報D1を埋め込む際に必要な公開鍵情報kpを秘密に管理する必要がなく、一般に自由に公開することができる。これにより、公開鍵情報kpの管理が容易で、誰でも自由に埋込情報D1の内容を確認することのできるシステムを構築することができる。また、原画像データGには、埋込情報D1を復元するための秘密情報D3を埋め込むため、原画像データGの著作権を十分に保護することもできる。

【0116】尚、上述した第2の実施の形態において、埋込装置100は、所定のファイルフォーマットに従って、公開鍵情報kpを電子透かし画像データG'に付加するようになされているものとする。例えば、画像データ部と画像ヘッダ部を含む画像ファイルフォーマットを採用する場合、電子透かし画像データG'を画像データ部に格納し、公開鍵情報kpを画像ヘッダ部に属性情報として格納する。このようなファイルフォーマットの構成については、後述する第4の実施の形態において詳細に説明する。

【0117】また、上述した第2の実施の形態では、電子透かし画像データG'に公開鍵情報kpを付加して、ネットワーク300に対して送出するものとしたが、これに限らず、例えば、電子透かし画像データG'と公開鍵情報kpをそれぞれ別情報として、それぞれで送出するようにしてもよい。

【0118】また、上述した第2の実施の形態において、埋込装置100から送出された公開鍵情報kpの正当性を検査するために、送信者自身の公開鍵暗号方式に基づくデジタル署名を公開鍵情報kpに対して施すような構成をとるようにしてもよい。この場合においても、公開鍵情報kpの秘密通信は必要ない。これにより、埋込情報D1の破壊や変更が難しくなり、安全性と信頼性とをより一層向上させたシステムを提供することができる。

【0119】（第3の実施の形態）本実施の形態では、上述した第2の実施の形態における埋込装置100と抽出装置200を用いて構成されるシステムを、例えば、図9に示すような構成のシステムに適用する。このシステムは、上述した第2の実施の形態でのシステム構成（上記図8参照）に加えて、鍵管理局500を更に含んだ構成としている。以下、本実施の形態でのシステムについて具体的に説明する。

【0120】尚、上記図9に示す本実施の形態でのシステムにおいて、第1又は第2の実施の形態でのシステムと同様の構成或いは機能を有する部分については同一の符号を付し、その詳細な説明を省略する。

【0121】まず、上記図9のシステムは、公衆回線、インターネット、イーサネット等からなる鍵管理局500を含んだネットワーク300を用いて構成されるシステムであって、例えば、静止画像データ、動画データ、音声データ、テキストデータ、グラフィックスデータ、プログラムデータなどのデジタルデータを配布したり、売買したりするデジタル情報配布システムや、電子商取引システムに適用されるものである。

【0122】そこで、本システムにおいては、上述した第2の実施の形態と同様にして、埋込装置100から送出された公開鍵情報kpの正当性を検査するために、送信者自身の公開鍵暗号方式に基づくデジタル署名を公開鍵情報kpに対して施すこともできるが、ここでは、鍵管理局500の公開鍵暗号方式に基づくデジタル署名を、埋込装置100から送出された公開鍵情報kpに対して施すように構成する。すなわち、鍵管理局500が、公開鍵情報kpの正当性を保証するように構成する。これにより、埋込情報D1の破壊や変更が難しくなり、安全性と信頼性とをより一層向上させたシステムを提供することができる。

【0123】上述のような構成をとることで、鍵管理局500は、公開暗号方式における認証局と同様の機能を有することになる。ここで、上記の“認証局”とは、公開暗号方式におけるユーザの公開鍵の正当性を保証するために、ユーザの公開鍵に証明書を発行する機関のことを言う。すなわち、認証局は、ユーザの公開鍵やユーザに関するデータに認証局の秘密鍵で署名を施すことによって証明書を作成して発行する。これにより、あるユーザから自分の証明書付き公開鍵を送られた他のユーザ

は、その証明書を認証局の公開鍵を用いて検査することによって、公開鍵を送ってきたユーザの正当性（少なくとも、認証局によって認められたユーザであること）を認証する。このような認証局を運営している組織としては、「VeriSign」やCyberTrust」等の企業がよく知られている。

【0124】したがって、鍵管理局500は、埋込装置100からネットワーク300に対して送出された公開鍵情報kpに対して、自分のデジタル署名を施し、これを公開鍵情報kp'として、抽出装置200に与えることになる。そして、抽出装置200は、鍵管理局300からの公開鍵情報kp'を用いて、埋込装置100からの電子透かし画像データG'から埋込情報D1を抽出する。

【0125】尚、上述した第3の実施の形態では、鍵管理局500にて署名が施された公開鍵情報kp'を、抽出装置200に与えるようにしたが、例えば、埋込装置100に対して与えるようにしてもよい。この場合、埋込装置100は、鍵管理局500からの公開鍵情報kp'を、電子透かし画像データG'と共に、抽出装置300にネットワーク300を介して与えるようにする。

【0126】また、上述した第3の実施の形態において、鍵管理局500を、例えば、不正配布の検査センター等として機能させるようにしてもよい。また、上述した第3の実施の形態において、埋込装置100から送出される電子透かし画像データG'を、例えば、暗号化されたデータとするようにしてもよい。

【0127】（第4の実施の形態）本実施の形態では、上述した第1～第3の実施の形態にける埋込装置100が、電子透かし画像データG'と公開鍵情報kpをネットワーク300に対して送出する際の、ファイルフォーマットとして、例えば、次のようなファイルフォーマットを採用する。

【0128】まず、通常の、一般的な画像ファイルフォーマットは、例えば、図10に示すようなフォーマット600で示される。これにより、埋込装置100は、ファイルフォーマット600に従って、送付する電子透かし画像データG'を画像データ部602に格納し、それに対する公開鍵情報kpを画像ヘッダ部601に格納する。一方、FlashPix™（“FlashPix”は米国EastmanKodak社の登録商標）ファイルフォーマットでは、詳細は後述するが、公開鍵情報kpと電子透かし画像データG'を、各階層のデータとして格納することができるようになされている。また、公開鍵情報kp等を属性情報として、プロパティセットの中に格納しておくこともできるようになされている。以下、一般的なファイルフォーマット、及びFlashPix™ファイルフォーマットについて具体的に説明する。

【0129】[一般的な画像ファイルフォーマット]

一般的な画像ファイルフォーマットは、上記図10に示したように、画像ファイルが画像ヘッダ部601と画像データ部602に分けられた構造としている。画像ヘッダ部601には、その画像ファイルから画像データを読み取るときに必要な情報や、画像の内容を説明する付帯的な情報が格納される。上記図10の例では、画像フォーマット名を示す画像フォーマット識別子、ファイルサイズ、画像の幅・高さ・深さ、圧縮の有無、解像度、画像データの格納位置のオフセット、及びカラーパレット、そして、公開鍵情報kp等の画像属性情報が格納されている。一方、画像データ部602には、画像データ自体が格納されている。このような画像ファイルフォーマットの代表的な例としては、Microsoft社のBMPフォーマットや、CompuServe社のGIFフォーマット等が広く普及している。

【0130】[FlashPix™ファイルフォーマット]以下に説明するFlashPix™ファイルフォーマットでは、上記図10に示した画像ヘッダ部601に格納される画像属性情報、及び画像データ部602に格納される画像データを、階層構造化して画像ファイル内に格納するようになされている。この階層構造化された画像ファイルフォーマットとしては、例えば、図11や図12に示すようなフォーマットがある。以下、これらの図11及び図12を用いて、FlashPix™ファイルフォーマットについて説明する。

【0131】まず、ファイル内の各プロパティやデータに対しては、MS-DOSのディレクトリとファイルに相当するストレージとストリームによってアクセスする。上記図11及び図12では、影付きブロックがストレージを示し、影無しブロックがストリームを示しており、画像データや画像属性情報（公開鍵情報kp等を含む情報）は、ストリーム部分に格納される。また、上記図12は、画像データが異なる解像度で階層化されて格納される様子を示しており、それぞれの解像度の画像を、ここでは“Subimage”と呼び、これらを“Resolution0, 1, . . . , n”で示している。そして、それぞれの解像度の画像に対して、対象画像データを読み出すために必要な情報が“Subimage Header”708に格納され、画像データが“Subimagedata”707に格納される。

【0132】上記図11及び図12に示す“Property Set”（プロパティセット）とは、画像属性情報を、その使用目的や内容に応じて分類して定義したものであり、このような“Property Set”としては、“Summary info. Property Set”701、“Image info. Property Set”704、“Image Content Property Set”703、“Extention list Property Set”705等がある。

【0133】上記図11及び図12に示す“Summary info. Property Set”701は、FlashPix™特有の

ものではなく、Microsoft社のストラクチャードストレージでは必須のものであり、画像ファイルのタイトル名、題名、著者、サムネール画像等が格納される。上記図11及び図12に示す“Comp Obj. Stream”702には、記録部(Storage)に関する一般的な情報が格納される。上記図11に示す“Image Content Property Set”703には、画像データの格納方法が記述される。例えば、図13に示すように、画像データの階層数、最大解像度の画像についての幅や高さ、それぞれの解像度の画像についての幅、高さ、色の構成、或いはJPEG圧縮方式を用いる際の量子化テーブル・ハフマンテーブルの定義等が記述される。上記図11及び図12に示す“Extention list Property Set”705は、FlashPix™の基本仕様に含まれない情報を追加格納する際に仕様する領域である。したがって、例えば、上述した第1～第3の実施の形態における公開鍵情報kpは、この“Extention list Property Set”705に格納されることになる。上記図11に示す“ICC Profile”706には、ICC (International Color Consortium)において規定される色空間変換のための変換プロファイルが記述される。

【0134】上記図11に示す“Image info. Property Set”704には、画像データを使用する際に利用できる次の(1)～(9)に示すような情報、すなわち、その画像がどのようにして取り込まれ、どのように利用可能であるか等の情報が格納される。

- (1) デジタルデータの取り込み方法、或いは生成方法に関する情報
 - (2) 著作権に関する情報
 - (3) 画像の内容（画像中に存在する人物や場所等）に関する情報
 - (4) 撮影に使用されたカメラに関する情報
 - (5) 撮影時のカメラのセッティング（露出、シャッタースピード、焦点距離、フラッシュ使用の有無等）の情報
 - (6) デジタルカメラ特有の解像度やモザイクフィルタに関する情報
 - (7) フィルムのメーカー名、製品名、種類（ネガ／ポジ、カラー／白黒等）等の情報
 - (8) オリジナル画像が書物や印刷物である場合の、その種類やサイズ等に関する情報
 - (9) スキャン画像の場合の、そのスキャンに使用したスキャナやソフト、操作した人等に関する情報
- 【0135】上記図12に示す“FlashPix Image View Object”は、画像を表示する際に用いるビューイングパラメータと画像データを合わせて格納する画像ファイルである。ここでのビューイングパラメータとは、画像の回転、拡大／縮小、移動、色変換、フィルタリング等の処理を、画像表示の際に適切にするために記憶しておく処理係数を示す。

【0136】上記図12に示す"Global Property set" 801には、ロックされている属性リストが記述され、例えば、最大画像のインデックスや、最大変更項目のインデックス、最終修正者に関する情報等が記述される。上記図12に示す"Source FlashPix Image Object" 802及び"Result FlashPix Image Object" 803は、FlashPix 画像データの実体である。"Source FlashPix Image Object" 802は、必須であり、オリジナルの画像データが格納される。一方、"Result FlashPix Image Object" 803は、オプションであり、ビューイングパラメータを使って画像処理した結果の画像データが格納される。上記図12に示す"Source desc. Property Set" 804及び"Result desc. Property Set" 805は、上記の画像データの識別のためのプロパティセットであり、画像ID、変更禁止のプロパティセット、最終変更日時等の情報が格納される。上記図12に示す"Transform Property Set" 806は、画像の回転、拡大/縮小、移動のためのAffine変換係数、色変換マトリクス、コントラスト調整値、フィルタリング係数等が格納される。

【0137】以上、本発明を適用した第1～第4の実施の形態について説明したが、本発明は、その精神、又は主要な特徴から逸脱することなく、他の様々な形で実施することができる。例えば、上述の実施の形態での埋込方法や抽出方法の一部或いは全てを、ソフトウェアの制御により処理することも可能である。例えば、上述した第1～第4の実施の形態での機能を実現するソフトウェアのプログラムコードを記録した記憶媒体（すなわち、上記図1や図7の記憶媒体106、上記図2の記憶媒体206）を、それぞれの実施の形態での装置（すなわち、上記図1や図7の埋込装置100、上記図2の抽出装置200）に供給するように構成する。また、上述した各実施の形態での装置が具備する制御部（すなわち、上記図1や図7の制御回路105、上記図2の制御回路205）が、上記記憶媒体に格納されたプログラムコードを読み出して実行することによっても、上述した各実施の形態での機能を実現することができる。この場合、上記記憶媒体から読み出されたプログラムコード自体が、上述した各実施の形態での機能を実現することになり、そのプログラムコードを記憶した記憶媒体は、本発明を構成することとなる。上記プログラムコードを供給するための記憶媒体としては、例えば、フロッピディスク、ハードディスク、光ディスク、光磁気ディスク、CD-ROM、CD-R、磁気テープ、不揮発性のメモリカード、ROMなどを用いることができる。また、上述した各実施の形態での制御部上で稼動しているOS（オペレーティングシステム）、或いはアプリケーションソフトウェア等が、上記記憶媒体から読み出されたプログラムコードの指示に基づき、実際の処理の一部或いは全てを実行することによっても、上述した各実施の形態で

の機能を実現することができる。さらに、上記記憶媒体から読み出されたプログラムコードが、上述した各実施の形態での制御部に接続された機能拡張ユニットの具備するメモリに書き込まれた後、その機能拡張ユニットに備わる制御部が、そのプログラムコードの指示に基づき、実際の処理の一部或いは全てを実行することによっても、上述した各実施の形態での機能を実現することができる。したがって、上述した第1～第4の各実施の形態では、あらゆる点で単なる例示に過ぎず、限定的に解釈してはならない。また、本発明の範囲は、特許請求の範囲によって示すものであって、明細書本文には何等拘束されない。さらに、特許請求の範囲の均等範囲に属する変形や変更は全て、本発明の範囲のものである。

【0138】

【発明の効果】以上説明したように本発明では、画像等のデジタルデータに対して、第1の情報（デジタルデータの著作権を管理したり保護するための著作権情報等）と、該第1の情報を復元するための第2の情報とを埋め込む。

【0139】具体的には例えば、公開された鍵情報（公開鍵情報）を用いて、著作権情報等の埋込情報（第1の情報、所定の情報：電子透かし等）をデジタルデータに対して目に見えないように埋め込むと共に、この埋込情報を復元するための秘密情報（第2の情報：例えば、誤り符号化処理により生成する場合にはパリティデータ）をも、公開されていない鍵情報（秘密鍵情報）を用いて、目に見えないように埋め込む。このとき、埋込対象となっているデジタルデータにおいて、埋込情報が埋め込まれた領域（第1の領域）と、秘密情報が埋め込まれた領域（第2の領域）と、それらの情報が埋め込まれていない領域（第3の領域）との間には、所定の関係がある。したがって、このようにして埋込情報及び秘密情報が共に埋め込まれたデジタルデータを受け取った側では、上記の公開された鍵情報を用いて、そのデジタルデータから埋込情報（著作権情報等）を自由に抽出することができる。これにより、一般のユーザは、外部から入手したデジタルデータの著作権の内容や、その正当性を確認することができる。また、デジタルデータに埋め込まれている埋込情報が、不正なユーザによって破壊或いは変更されていたとしても、その埋込情報と共に埋め込まれている秘密情報によって、該埋込情報を復元することができるため、デジタルデータの著作権を十分に保護することができ、埋込情報の信頼性と安全性を共に向上させることもできる。

【0140】よって、本発明によれば、埋込情報の抽出に必要な鍵情報を秘密に管理することなく、一般のユーザによる自由な埋込情報の抽出と、デジタルデータの著作権の保護とを同時に満たすことのできる著作権保護技術を提供することができる。このような本発明による技術は、特に、電子商取引システムやデジタル情報配

布システム等に適用して有効である。

【図面の簡単な説明】

【図 1】第 1 の実施の形態において、本発明を適用したシステムの埋込装置の構成を示すブロック図である。

【図 2】上記システムの抽出装置の構成を示すブロック図である。

【図 3】上記埋込装置にて実行される埋込方法を説明するためのフローチャートである。

【図 4】上記埋込方法において、原画像に対する情報の埋め込みを説明するための図である。

【図 5】上記抽出装置にて実行される抽出方法を説明するためのフローチャートである。

【図 6】上記埋込方法及び上記抽出方法の応用例 1 を説明するための図である。

【図 7】上記埋込方法及び上記抽出方法の応用例 3 を説明するための図である。

【図 8】第 2 の実施の形態における上記システムの構成を示すブロック図である。

【図 9】第 3 の実施の形態における上記システムの構成を示すブロック図である。

【図 10】第 4 の実施の形態において、上記システムにて用いる画像ファイルフォーマットとしての、一般的な画像ファイルフォーマットを説明するための図である。

【図 11】上記システムにて用いる画像ファイルフォーマットとしての、階層構造化された画像ファイルフォー

マットを説明するための図である。

【図 12】上記システムにて用いる画像ファイルフォーマットとしての、他の階層構造化された画像ファイルフォーマットを説明するための図である。

【図 13】上記階層構造化された画像ファイルフォーマットに格納される、画像データの格納方法についての情報の一例を説明するための図である。

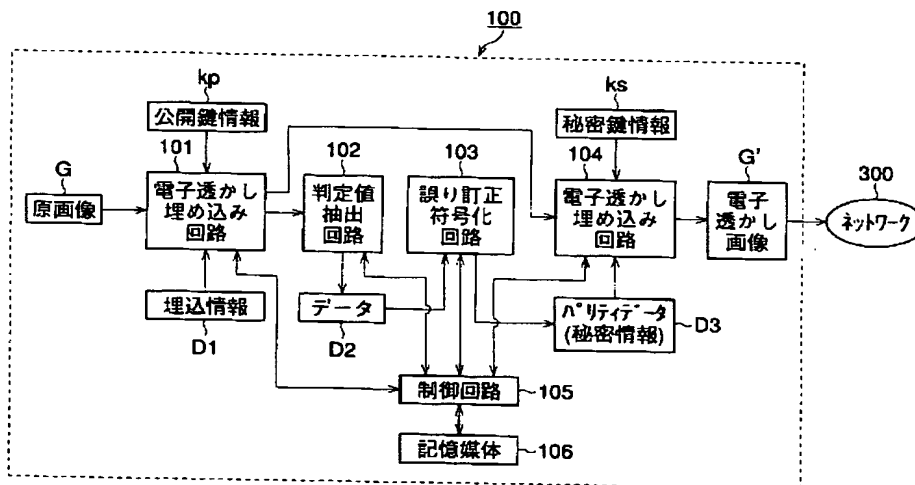
【図 14】従来の電子透かし技術を用いたシステムの構成を示すブロック図である。

10 【符号の説明】

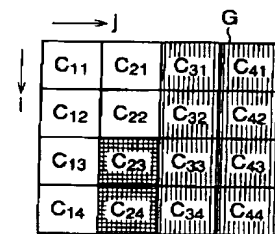
- 100 埋込装置
- 101 電子透かし埋込回路
- 102 判定値抽出回路
- 103 誤り訂正符号化回路
- 104 電子透かし埋込回路
- 105 制御回路
- 106 記憶媒体
- 200 抽出装置
- 201 電子透かし抽出回路
- 202 誤り訂正復号回路
- 203 電子透かし抽出回路
- 204 表示部
- 205 制御部
- 206 記憶媒体
- 300 ネットワーク

20

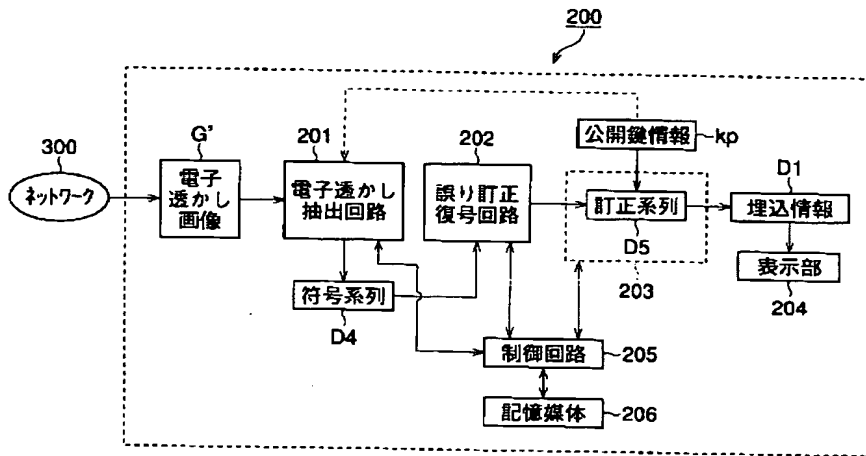
【図 1】



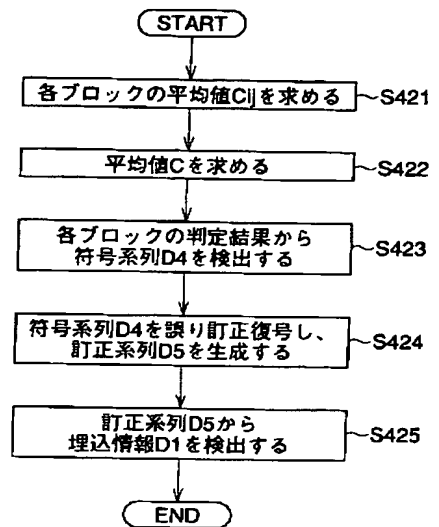
【図 4】



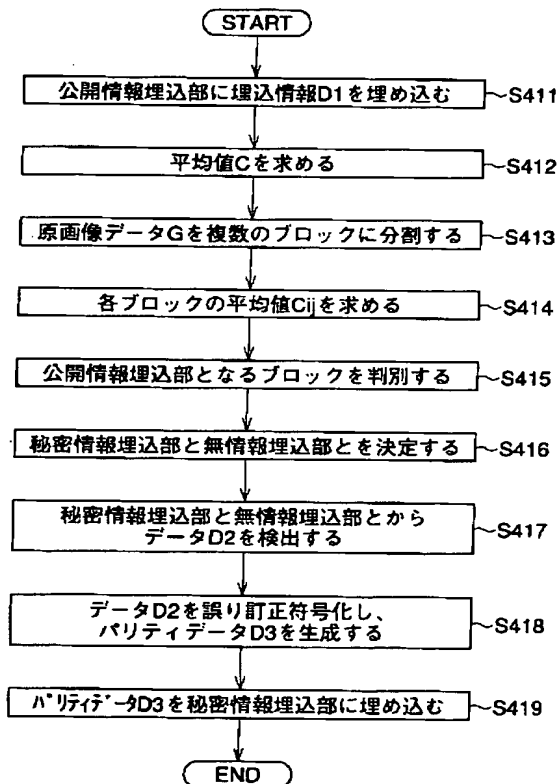
【図 2】



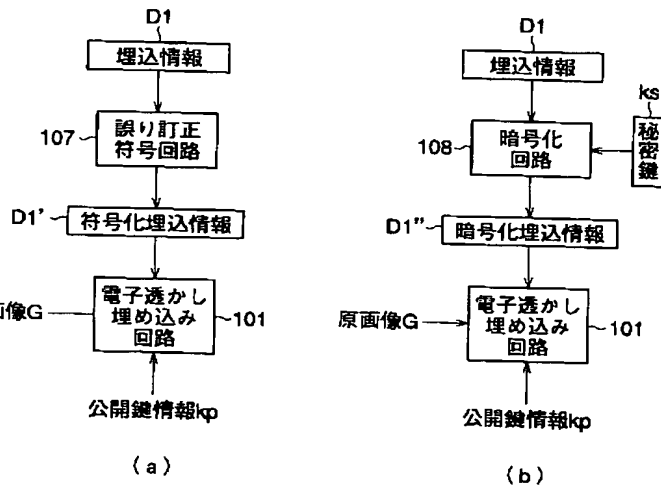
【図 5】



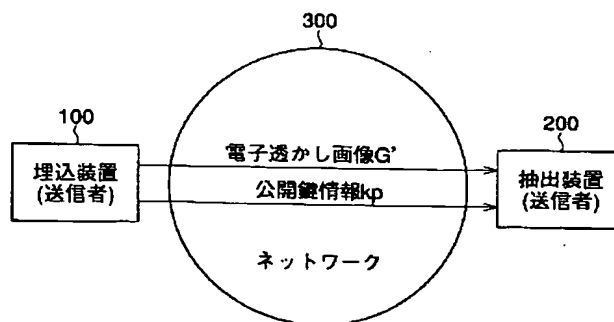
【図 3】



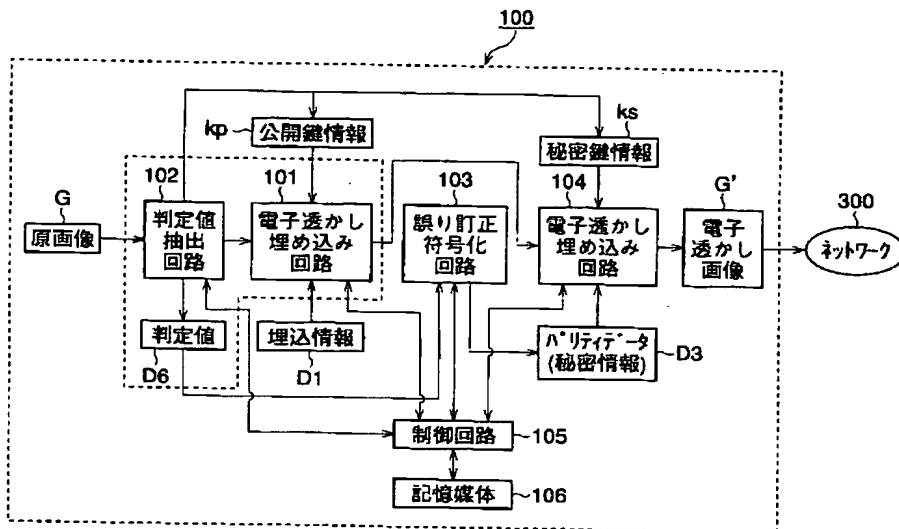
【図 6】



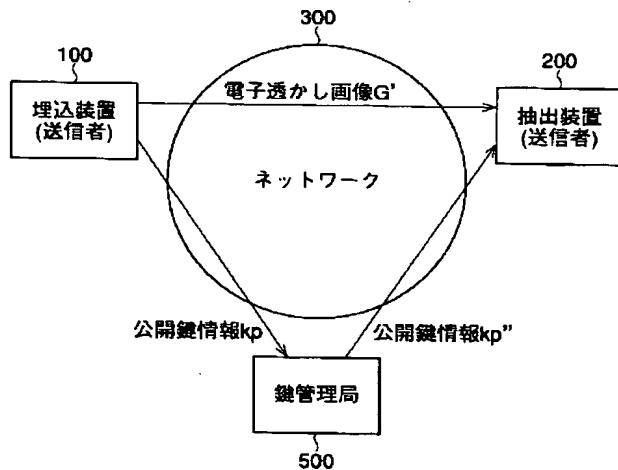
【図 8】



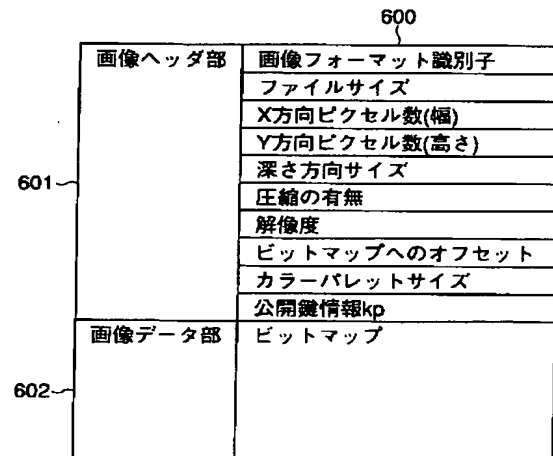
【図 7】



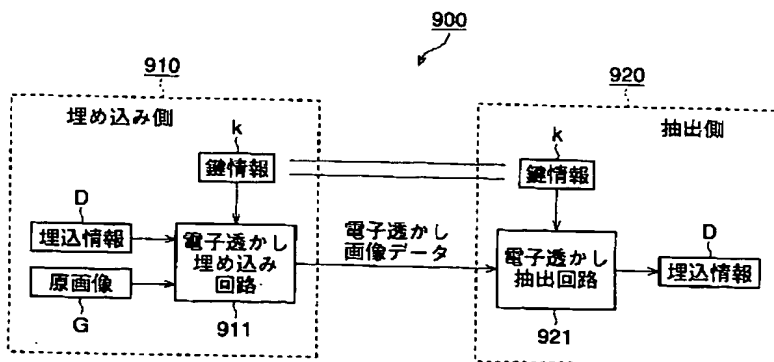
【図 9】



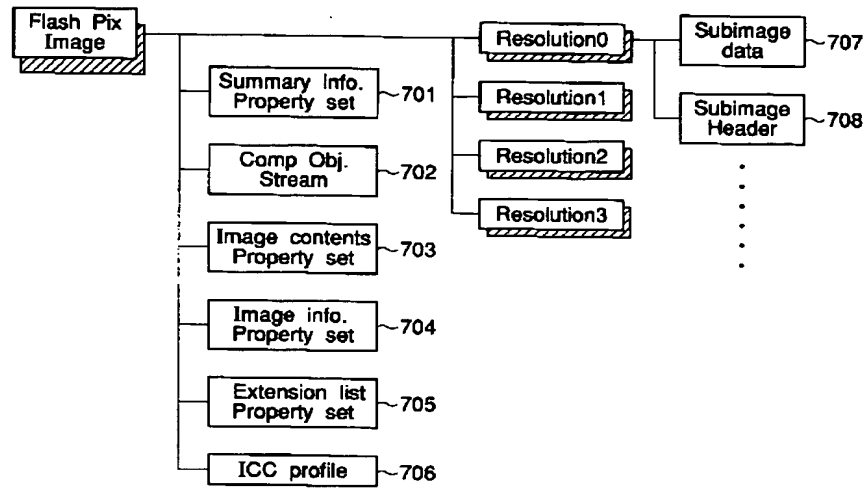
【図 10】



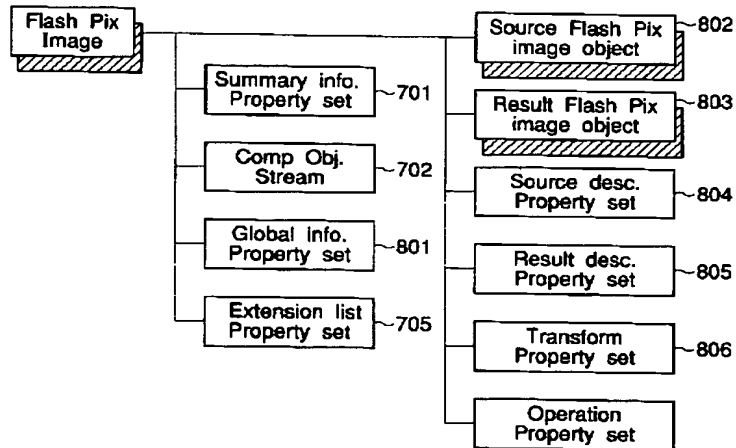
【図 14】



【図 1 1】



【図 1 2】



【図13】

プロパティ名	IDコード	タイプ
画像データの階層数	0x01000000	VT_UI4
最大解像度の画像の幅	0x01000002	VT_UI4
最大解像度の画像の高さ	0x01000003	VT_UI4
初期表示の高さ	0x01000004	VT_R4
初期表示の幅	0x01000005	VT_R4

プロパティ名	IDコード	タイプ
各解像度の画像の幅	0x02110000	VT_UI4
各解像度の画像の高さ	0x02110001	VT_UI4
各解像度の画像の色	0x02110002	VT_BLOB
各解像度の画像を数値で表わしたフォーマット	0x02110003	VT_UI4 VT_VECTOR

プロパティ名	IDコード	タイプ
JPEGテーブル	0x03110001	VT_BLOB
最大JPEGテーブルのインデックス	0x03000002	VT_UI4